

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by
name and address)
THE ELECTRONIC DEVICES SEIZED FROM A LAPTOP BAG
ASSOCIATED WITH ROBERT WESLEY ROBB CURRENTLY IN
FBI CUSTODY IN MANASSAS, VIRGINIA

Case No. 1:24-SW-222

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

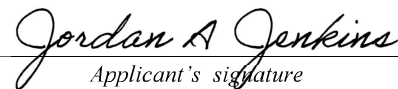
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1343 (Wire Fraud), 1956(a)(1)(B)(ii) (Concealment Money Laundering), and 1957 (Unlawful Monetary Transactions).	

The application is based on these facts:

SEE AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Jordan Jenkins, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 04/01/2024

City and state: Alexandria, Virginia

 Digitally signed by Ivan Davis
Date: 2024.04.01 13:40:45 -04'00'
Judge's signature

Hon. Ivan D. Davis, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched are the **SUBJECT DEVICES** currently located at the Federal Bureau of Investigation, Washington Field Office, Northern Virginia Resident Agency, in Manassas, Virginia, including:

- a. one SanDisk thumb drive (Device 1);
- b. one Rog Strix Arion External Hard Drive (Device 2);
- c. one HP Envy laptop with serial number 8CG114H0W1 (Device 3);
- d. one Predator Helios Neo 16 laptop with serial number NGQMAAA0013140C5E77600 (Device 4);
- e. one Apple iPad with serial number GG7FK29GQ16K (Device 5); and
- f. one silver Apple iPhone (Device 6)

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

List of Items to be Seized and Searched

Items constituting fruits, evidence, or instrumentalities of violations of the Specified Federal Offenses including but not limited to the following:

1. Records and information relating to cryptocurrency, trading bots, and financial activity;
2. All bank records, checks, credit card bills, account information, and other financial records, including records pertaining to cryptocurrency accounts and/or wallets and information such as seed phrases that may be used to reconstitute or access those wallets to examine their contents;
3. All communications concerning the above-described investment scheme, including, but not limited to, references to a cryptocurrency trading bots, investment opportunities, the disposition of investor funds, and the transfer and use of cryptocurrency and funds related to the investment scheme;
4. Records and information relating to the development of a MEV cryptocurrency trading bot, including whether such a bot actually exists;
5. Records and information related to the laundering and disposition of investor funds, including potential assets representing the proceeds of the Specified Federal Offenses or property involved in the Specified Federal Offenses;
6. Internet usage records, user names, logins, passwords, e-mail addresses, and identities assumed for purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;

7. Address books, names, and lists of names and address of individuals who may have been contacted by the computer and internet websites;

8. Records and information relating to membership in online groups, social media platforms, and encrypted communication applications;

9. Records and information relating to any online storage or communication accounts used to communicate about and effectuate the Specified Federal Offenses;

10. Records and information that constitute evidence of the state of mind of ROBB, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;

11. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with ROBB about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts; and

12. Evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

13. Evidence of software, or the lack thereof, that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

14. Evidence indicating how and when the SUBJECT DEVICES were accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

15. Evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

16. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICE;

17. Evidence of the times the SUBJECT DEVICES were used;

18. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES or programs on the SUBJECT DEVICES;

19. Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;

20. Records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

21. contextual information necessary to understand the evidence described in this attachment.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.